VMware ESXi Administration Guide

FortiAnalyzer 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

Apr 11, 2022
FortiAnalyzer 7.2.0 VMware ESXi Administration Guide
05-720-0794621-20220411

TABLE OF CONTENTS

Change log **4**
About FortiAnalyzer on VMware ESXi **5**
Licensing 5
Trial license 5
Add-on license 6
Preparing for deployment **7**
Minimum system requirements 7
Deployment package for VMware ESXi 8
Downloading a deployment package 8
Deployment **10**
Deploying FortiAnalyzer on VMware vSphere 10
Deploying the OVF file 10
Configuring hardware settings 13
Powering on the VM 14
Configuring initial settings 15
Enabling GUI access 15
Connecting to the GUI and enabling a trial license 16
Upgrading to an add-on license 16
Configuring your FortiAnalyzer 16

Change log

Date	Change description
2022-04-11	Initial release.

About FortiAnalyzer on VMware ESXi

This document provides information about deploying a FortiAnalyzer virtual appliance in VMware vSphere Hypervisor (ESX/ESCi) and VMware vSphere Client environments.

This includes how to configure the virtual appliance's virtual hardware settings. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuring and operating the virtual appliance after successfully installing and starting it. For that information, see the *FortiAnalyzer Administration Guide*.

Licensing

Fortinet offers the FortiAnalyzer-VM with a limited, free trial license. Stackable licenses can be purchased, letting you expand your VM solution as your environment expands. You can purchase perpetual or subscription-based licenses. Perpetual licenses never expire.

For information on purchasing a FortiAnalyzer-VM license, contact your Fortinet-authorized reseller, or visit How To Buy.

When configuring your FortiAnalyzer-VM, ensure that you configure hardware settings as the following table outlines and consider future expansion. Contact your Fortinet-authorized reseller for more information.

License	GB/day of logs	Minimum storage capacity
Trial License	1	500 GB
VM-GB1	+1	+500 GB
VM-GB5	+5	+3 TB
VM-GB25	+25	+10 TB
VM-GB100	+100	+24 TB
VM-GB500	+500	+48 TB
VM-GB2000	+2000	+100 TB

See Minimum system requirements on page 7.

See also the FortiAnalyzer product datasheet.

Trial license

With a FortiCare account, FortiAnalyzer-VM includes a free limited non-expiring trial license.

The free trial license includes support for 3 ADOMs and 1 GB/day of logs with 500GB of storage.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiAnalyzer-VM. Full-feature products and services are available for purchase with an add-on license. See Connecting to the GUI and enabling a trial license on page 16.

Add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Deployment package for VMware ESXi on page 8
- Downloading a deployment package

Minimum system requirements

The following table lists the minimum system requirements for your VM hardware, based on your VM's analytic sustained rate.

Analytic sustained rate (logs/sec)	VM hardware requirements		
	RAM (GB)	CPU cores	IOPS
3000	8	4	300
4000	8	4	400
5000	8	4	500
6000	16	8	600
7000	16	8	700
8000	16	8	800
9000	16	8	900
10000	16	8	1000
20000	32	16	2000
30000	32	16	3000
40000	64	32	4000
50000	64	32	5000

You can calculate the collector sustained rate by multiplying the analytic sustained rate by 1.5.

This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.

Deployment package for VMware ESXi

Firmware images on the Customer Service & Support site include FortiAnalyzer-VM deployment packages. The following table lists the available VM deployment package:

VM platform	Deployment file
VMware ESXi	ESX/ESXi server: `FAZ_VM64-vX-buildxxxx-FORTINET.out.ovf.zip`

For the latest information on virtualization software support, see the corresponding FortiAnalyzer Release Notes on the Fortinet Docs Library.

The `.out.ovf.zip` file contains:

File	Description
`DATADRIVE.vmdk`	FortiAnalyzer-VM log disk in VMDK format.
`FAZ.vmdk`	FortiAnalyzer system hard disk in Virtual Machine Disk (VMDK) format.
`FortiAnalyzer-VM64.hw14.ovf`	OVF template file for VMware ESXi 6.7 and later versions.
`FortiAnalyzer-VM64.hw14.vapp.ovf`	OVF template file for VMware vSphere, vCenter, and vCloud (ESXi 6.7 and later).
`FortiAnalyzer-VM64.ovf`	OVF template based on Intel e1000 NIC driver.
`FortiAnalyzer-VM64.vapp.ovf`	OVF template file for VMware vSphere, vCenter, and vCloud (earlier than ESXi 6.7).

For more information about FortiAnalyzer, see the FortiAnalyzer datasheet.

Downloading a deployment package

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention. Each firmware image is specific to the device model. For example, the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64-bit Microsoft Hyper-V Server virtualization environment.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiAnalyzer* > *Download* tab.

Download the `.out` file to upgrade your existing FortiAnalyzer installation.

To download deployment packages:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiManager* from the *Select Product* dropdown list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Deployment

Prior to deploying the FortiAnalyzer, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer presume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiAnalyzer appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiAnalyzer, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiAnalyzer GUI (see Enabling GUI access on page 15).

If the FortiAnalyzerdoes not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

Deploying FortiAnalyzer on VMware vSphere

After you download the `FAZ_VM64-vx-buildxxxx-FORTINET.out.ovf.zip` file and extract the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiAnalyzer-VM, ensure that you configure the following and they are functioning properly:

- You must install VMware vSphere Hypervisor™ (ESX/ESXi) software on a server and update it to the latest patch release prior to installing FortiAnalyzer. Go to What is a vSphere Hypervisor? for installation details.
- You must install VMware vSphere Client™ on the computer that you will use for managing the FortiAnalyzer-VM.

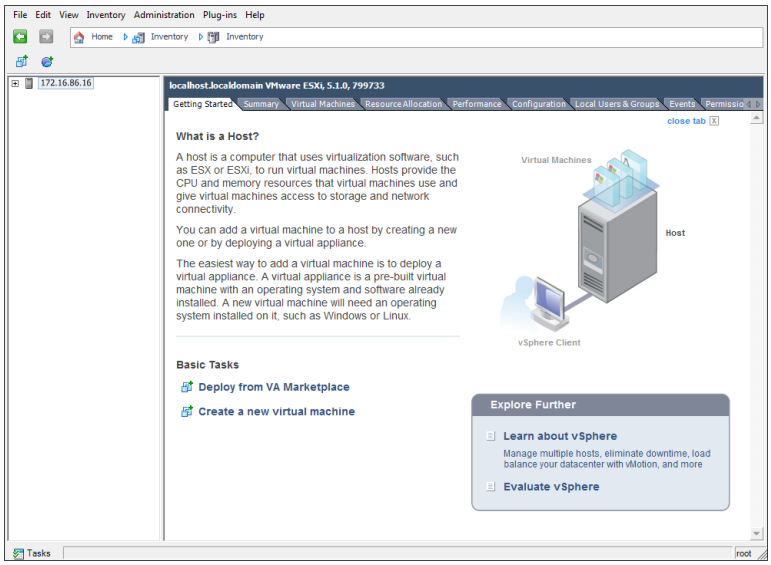
This section includes the following topics:

- Deploying the OVF file
- Configuring hardware settings
- Powering on the VM

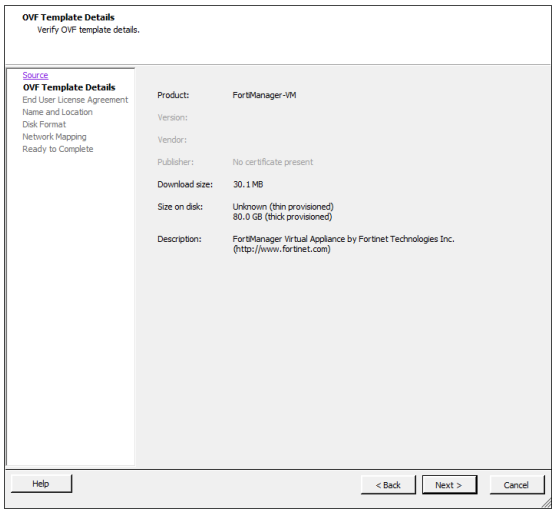
Deploying the OVF file

To deploy the OVF file template:

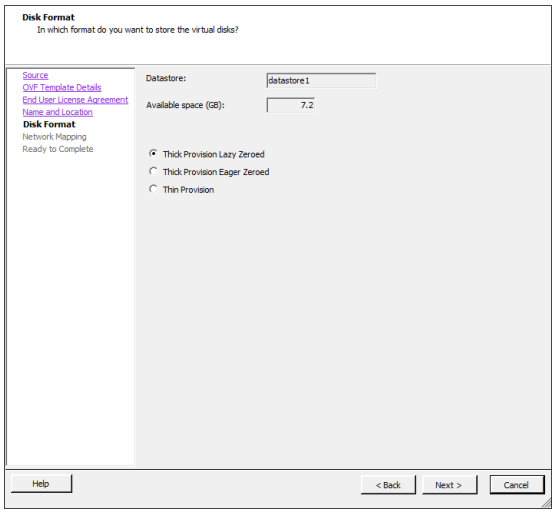
1. Launch the VMware vSphere client, enter your server's IP address or hostname, your username, and password, then click *Login*. The vSphere client homepage opens.



2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard. The OVF Template *Source* page opens.
3. Configure the FortiAnalyzer-VM using the OVF Template wizard:
   a. Click *Browse*, locate the OVF file on your computer, then click *Next* to continue. The OVF Template *Details* page opens.



   b. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Click *Next* to continue. The OVF Template *End User License Agreement* page opens.
   c. Read the end user license agreement, then click *Accept* then *Next* to continue. The OVF Template *Name and Location* page opens.
   d. Enter a name for this OVF template. The name can contain up to 80 characters and must be unique within the inventory folder. Click *Next* to continue. The OVF Template *Disk Format* page opens.

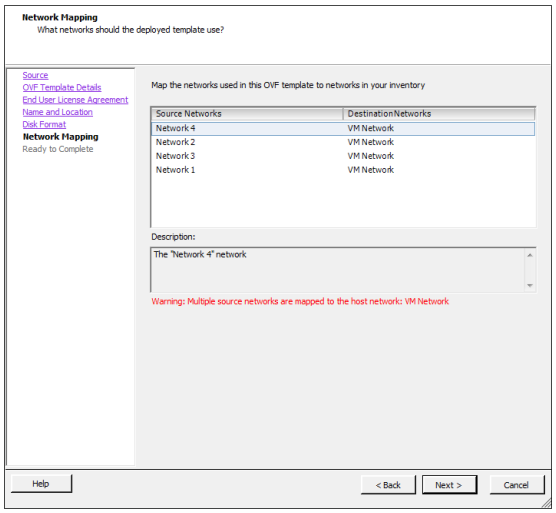


e. Select one of the following:

- *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
- *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
- *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the Virtual Machine File System (VMFS) reports the total volume size to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data.

If you know your environment will expand in the future, adding hard disks larger than the FortiAnalyzer base license requirement and utilizing *Thin Provision* when setting the OVF Template disk format is recommended. This allows your environment to expand as required while not taking up more space in the SAN than needed.

f. Click *Next* to continue. The OVF Template *Network Mapping* page opens.



g. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiAnalyzer. You must set the destination network for this entry to access the device console. Click *Next* to continue. The OVF Template *Ready to Complete* page opens.

4. Review the template configuration. Ensure that *Power on after deployment* is not enabled. You may need to configure the FortiAnalyzer hardware settings prior to powering on the VM.
5. Click *Finish* to deploy the OVF template. A *Deployment Completed Successfully* dialog displays once the FortiAnalyzer OVF template wizard has finished.

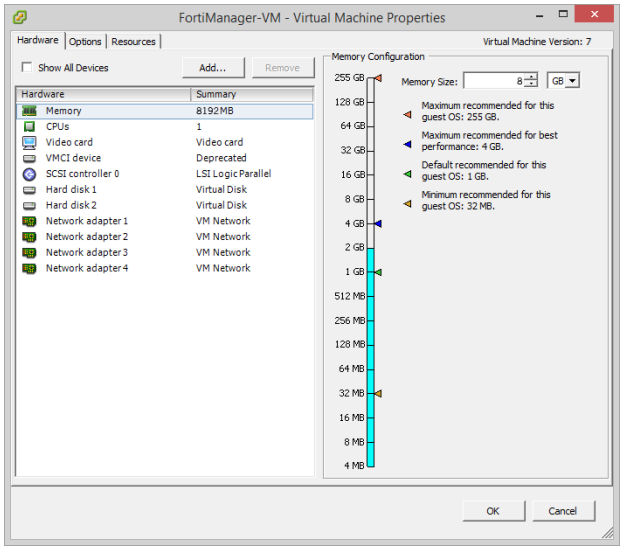
Configuring hardware settings

Before powering on your FortiAnalyzer-VM, you must configure the virtual memory, virtual CPU, and virtual disk.

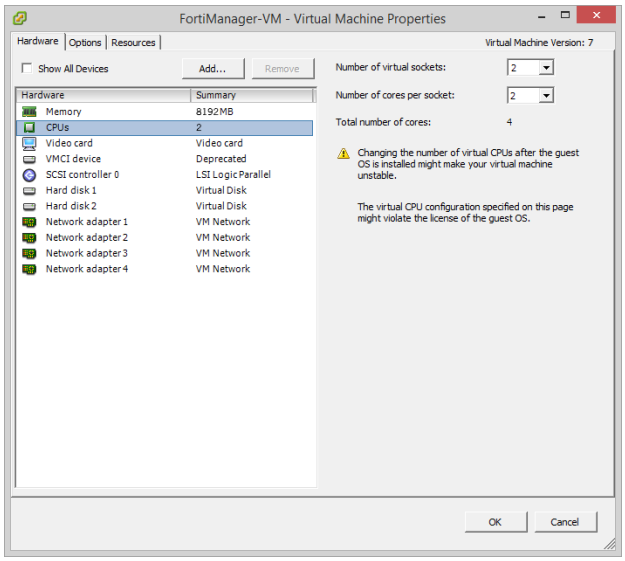
In FortiAnalyzer 5.6 and later, the network interface mapping has changed. See the *FortiAnalyzer Upgrade Guide* for more information.

To configure hardware settings:

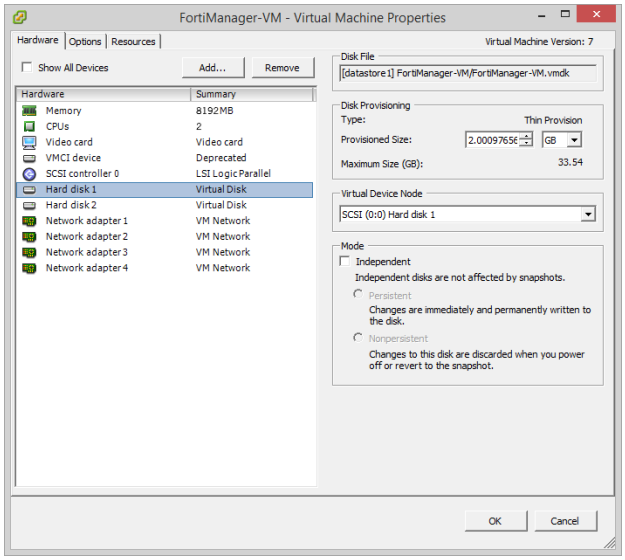
1. In the vSphere Client, right-click the FortiAnalyzer-VM in the left pane, and select *Edit Settings* to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. See Minimum system requirements on page 7 to determine your required memory.



3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.



4. Select *Hard disk 2*, the log disk, from the *Hardware* list, and configure it as required. You should not edit *Hard disk 1*.



The FortiAnalyzer-VM allows you to add twelve virtual log disks to a deployed instance. When adding additional hard disks, use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

5. Click *OK* to apply your changes.

Powering on the VM

You can now proceed to power on your FortiAnalyzer.

- Select the FortiAnalyzer in the left pane, then click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.

- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

Once the VM starts, proceed with the initial configuration. See Configuring initial settings on page 15.

Configuring initial settings

Before you can connect to the FortiAnalyzer-VM, you must configure basic network settings via the CLI console. Once configured, you can connect to the FortiAnalyzer GUI.

Enabling GUI access

To enable GUI access to the FortiAnalyzer, you must configure the IP address and network mask of the appropriate port on the FortiAnalyzer. The following instructions use port 1.

You can determine the appropriate by matching the network adapter's MAC address and the `HWaddr` that the CLI command `diagnose fmnetwork interface list` provides.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiAnalyzer and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiAnalyzer login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
config system interface
   edit port1
      set ip <IP address> <netmask>
end
```

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor VM settings.

4. To configure the default gateway, enter the following commands:

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

The Customer Service & Support portal does not currently support IPv6 for FortiAnalyzer license validation. You must specify an IPv4 address in the support portal and the port management interface.

Connecting to the GUI and enabling a trial license

Once you have configured a port's IP address and network mask, you can connect to the GUI by using a web browser.

To connect to the GUI and enable a trial license:

1. Launch a web browser, and enter the IP address you configured for the port management interface.
2. At the login page, select *Free Trial*, and click *Login with FortiCloud* to start the process of activating your free trial license.
   If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Upgrading to an add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Configuring your FortiAnalyzer

Once the FortiAnalyzer license has been validated, you can configure your device.

If the amount of memory or number of CPUs is too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages show in the GUI in the *System Resources* widget on the dashboard and in the *Notification* list.

www.fortinet.com